eco – AK Sicherheit

Rechtliche Stellung des CISO
- Handlungsrahmen und –pflichten -

Köln, 3. September 2008

Jens Eckhardt
JUCONOMY Rechtsanwälte
Düsseldorf

CISO – Eine Positionsbestimmung

- Aussagen zum CISO

  - „ *Der CISO ist … Prediger, Geheimagent und Notarzt.*“ (Quelle: www.computerwoche.de, Simon Hülsbömer)
  - „*Sicherheitsverantwortliche agieren gespalten: sie müssen Sicherheitsrisiken eingehen, um insgesamt für eine stabilere Sicherheitskultur zu sorgen.*“ (www.cio.de, Alexander Galdy)
  - „*CISOs werden als Vertreter einer anderen, unbekannten und unfassbaren Welt mit eigener Sprache und Ordnung betrachtet.*“ (www.cio.de, Alexander Galdy)
  - „*Die CISOs kümmern sich weniger um das Tagesgeschäft der IT, sondern sind zunehmend in langfristigen Geschäftsentscheidungen involviert.*“ (www.cio.de, Ingo Butters)

  ⇂ kein faktisch eindeutiges Berufsbild/Tätigkeitsbeschreibung

Aufgaben, Pflichten und Rechte des CISO

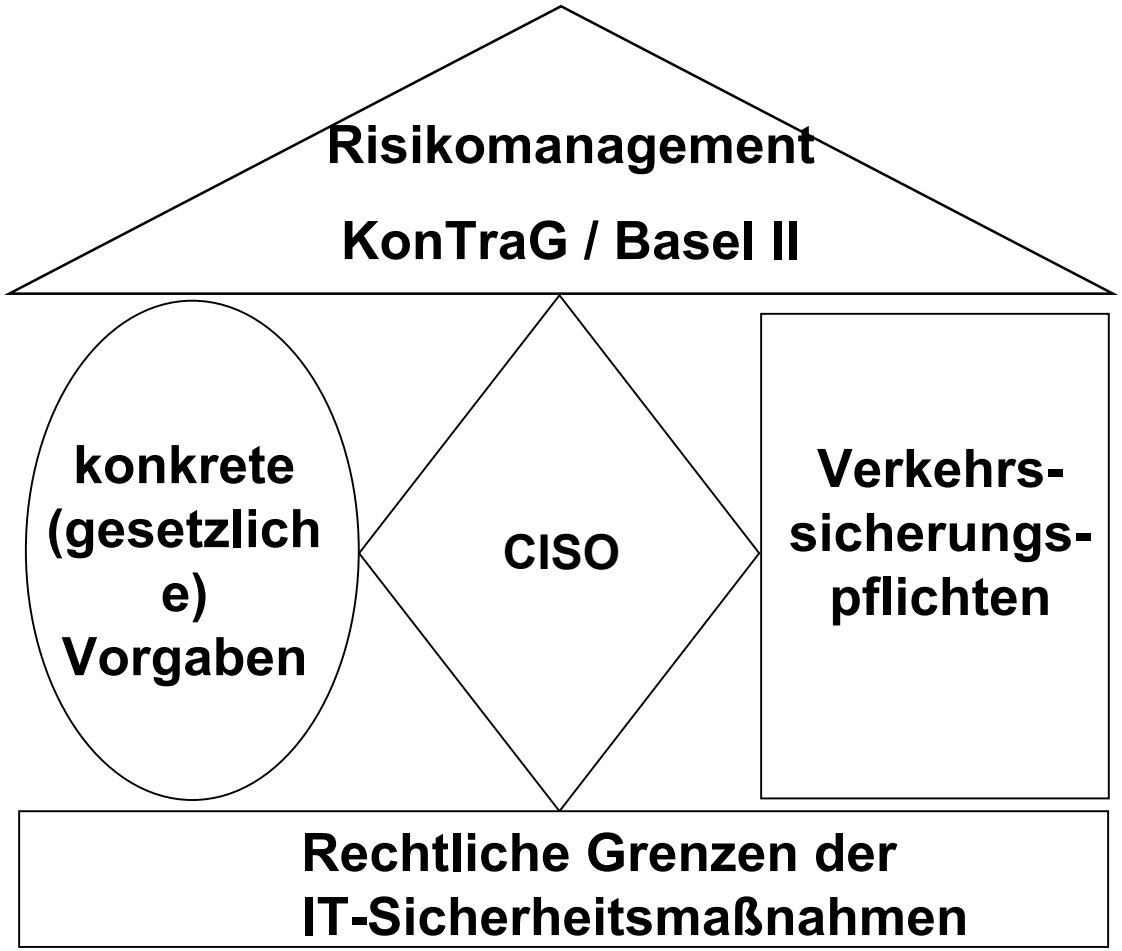
- Betrieblicher Datenschutzbeauftragter
  - Pflicht zur Bestellung (§ 4f BDSD)
  - gesetzliche Aufgabenbeschreibung (§ 4g BDSG)
- IT-Sicherheitsbeauftragter
  - grds. keine Pflicht zur Bestellung
  - bestimmte Untern. (z. B. § 109 TKG): Pflicht zur Bestellung
  - kein gesetzlich bestimmtes Aufgabenfeld
  - Erarbeitung, Pflege und Kontrolle der IT-Sicherheit (Konzept)
  - nicht gesetzlich geregelt: Weisungsrecht und -pflicht oder Berichtsrecht und -pflicht
- Vorstand/Geschäftsführung des Unternehmens
  - gesetzliche Pflichten und Rechte im Gesetz – je nach Rechtsform – jedenfalls in Grundzügen geregelt
  - u. a. Risikomanagement (verdeutlicht durch KontraG) und IT-Sicherheit (insbes. § 9 BDSG plus Anlage („via“ Bußgeldbestimm.))

Aufgaben, Pflichten und Rechte des CISO

- „Das deutsche Recht kennt den CISO (noch) nicht!“
- Festlegung durch Arbeitsvertrag/Stellenbeschreibung erforderlich
  - Eckpunkte der möglichst konkreten Beschreibung
    - Aufgaben
    - Kontrollrechte
    - Weisungsrechte
    - Berichtspflichten(/-rechte) gegenüber der Geschäftsführung
  - CISO ≠ IT-Sicherheitsbeauftragter ?
    - CISO: langfristige Geschäftsentscheidungen
    - IT-Sicherheitsbeauftragter: Tagesgeschäft
  - Berücksichtigung der gesetzlichen Rahmenbedingungen bei der Festlegung der Tätigkeit

Aufgaben, Pflichten und Rechte des CISO

- Gesetzlichen Rahmenbedingungen der IT-Sicherheit im Überblick
  - IT-Sicherheit – gesetzlich nicht definiert
    - Umschreibung: *Sicherheit in der IT bedeutet die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen in 1. informationstechnischen Systemen oder Komponenten oder 2. bei der Anwendung von informationstechnischen Systemen oder Komponenten.*
    - CISO: zusätzlich physische Sicherheit ?
  - Technische Regelwerke und Organisationsmodelle (Bsp.: ISO 17799; BS 7799; Grundschutzhandbuch des BSI; ITSEC/CC)
    - (nur?) faktische Verbindlichkeit als Haftungsmaßstab
  - § 9 BDSG nebst Anlage: techn. und organisator. Maßnahmen
  - Sektorspezifisches (z. B. § 109 TKG, § 25a KWG, §§ 33 ff WpHG)
  - „Verkehrssicherungspflichten“ für „Gefahrenquellen“
  - Buchführungspflichten (GoB, GobS, GDPdU)
  - CISO: zusätzlich Risikomanagement (Basel II und/oder KonTraG)?
  - Grenzen: Datenschutz (Fernmeldegeh) und betriebl


Risikomanagement
KonTraG / Basel II
konkrete (gesetzliche) Vorgaben
CISO
Verkehrs-sicherungs-pflichten
Rechtliche Grenzen der IT-Sicherheitsmaßnahmen

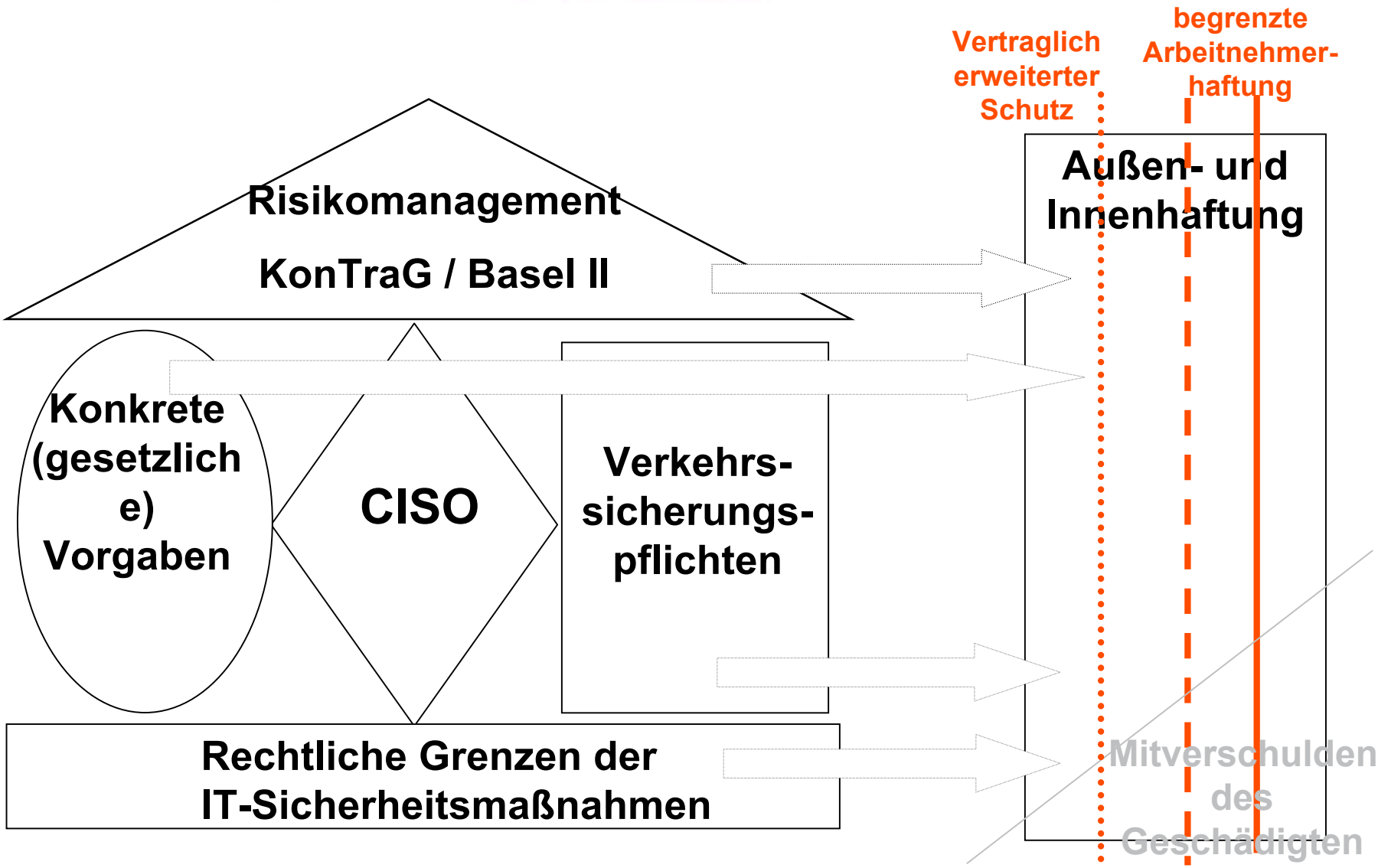
Haftung des CISO

- Außenhaftung (d. h. gegenüber dem externen Geschädigten)
  - CISO für sein Fehlverhalten
  - allgemeine Gesetze (§§ 823, 831 BGB)
  - Spezialregelungen: bspw. §§ 7, 9 BDSG, § 44 TKG
  - grds. keine Haftungsbegrenzung im Außenverhältnis (Ausnahme bspw. TK-Sektor)
  - Freistellungsanspruch entsprechend arbeitsrechtliche Haftungsbegrenzung
- Innenhaftung (d. h. gegenüber dem intern (mittelbar) Geschädigten)
  - CISO für sein Fehlverhalten
    - Relevanz der Tätigkeitsbeschreibung
    - Organisationsfehler
  - CISO als leitender Angestellter für „seine“ Mitarbeiter
    - Organisations- und Auswahlverschulden
  - CISO als Vorstand

Haftung des CISO

- Begrenzung der Haftung aufgrund Arbeitnehmerstellung
  - Wirkung der Haftungsbegrenzung
    - \ Freistellungsanspruch bei Außenhaftung
    - \ Haftungsbegrenzung bei Innenhaftung
  - Quotelung
    - leichte Fahrlässigkeit: keine Haftung
    - mittlere Fahrlässigkeit: Quotelung
    - Vorsatz/grobe Fahrlässigekeit: uneingeschränkte Haftung

    \ vertragliche Verbesserungen erforderlich, da CISO „Handlungsspielräume“ benötigt
  - Besonderheit: Haftung des CISO als Vorstand (bspw. § 91 Abs. 2 AktG / keine vollständige Befreiung durch Delegation)
- Haftungsmaßstab
  - rechtliche Vorgaben
  - Techn. Regelwerke/Stand der Technik und Organisationsmodelle


Vertraglich erweiterter Schutz
begrenzte Arbeitnehmer-haftung
Risikomanagement
KonTraG / Basel II
Außen- und Innenhaftung
Konkrete (gesetzliche) Vorgaben
CISO
Verkehrs-sicherungs-pflichten
Rechtliche Grenzen der IT-Sicherheitsmaßnahmen
Mitverschulden des Geschädigten

1	CISO – Eine Positionsbestimmung
2	Aufgaben, Pflichten und Rechte des CISO
3	Haftung des CISO
4	Diskussion und Fragen

Diskussion
und
Ihre Fragen

JUCONOMY Rechtsanwälte
Graf-Recke-Straße 82
40239 Düsseldorf
Tel. 0211 90 99 16 65 / 0178 666 40 60
E-Mail: eckhardt@juconomy.de

Kostenloser monatlicher Newsletter unter: www.juconomy.de